MAIL STOP APPEAL
BRIEF - PATENTS

AF
JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	H. Koike et al.	Attorney Docket No. NAII116493
Application No.:	09/710,203	Art Unit: 2131 Confirmation No.: 4596
Filed:	November 9, 2000	Examiner: K. Abrishamkar
Title:	LOG FILE PROTECTION SYSTEM	

TRANSMITTAL OF APPEAL BRIEF

September 23, 2005

TO THE COMMISSIONER FOR PATENTS:

Enclosed herewith for filing in the above-identified application is an Appeal Brief. Also enclosed is our Check No. 166310 in the amount of $250.00. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16, 1.17 and 1.18 which may be required during the entire pendency of the application, or credit any overpayment, to Deposit Account No. 03-1740. This authorization also hereby includes a request for any extensions of time of the appropriate length required upon the filing of any reply during the entire prosecution of this application. A copy of this sheet is enclosed.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS[PLLC]

Shoko I. Leek
Registration No. 43,746
Direct Dial No. 206.695.1780

I hereby certify that this correspondence is being deposited with the U.S. Postal Service in a sealed envelope as first class mail with postage thereon fully prepaid and addressed to Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the below date.

Date: September 23, 2005

SIL:jmb

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

MAIL STOP APPEAL
BRIEF - PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants:	H. Koike et al.	Attorney Docket No. NAII116493
Application No:	09/710,203	Art Unit: 2131 Confirmation No.: 4596
Filed:	November 9, 2000	Examiner: K. Abrishamkar
Title:	LOG FILE PROTECTION SYSTEM	

APPELLANT'S APPEAL BRIEF

Seattle, Washington

September 23, 2005

TO THE COMMISSIONER FOR PATENTS:

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

TABLE OF CONTENTS

		Page
I.	REAL PARTY IN INTEREST	1
II.	RELATED APPEALS AND INTERFERENCES	2
III.	STATUS OF CLAIMS	3
IV.	STATUS OF AMENDMENTS	4
V.	SUMMARY OF CLAIMED SUBJECT MATTER	5
	Claim 1	5
	Claim 26	6
VI.	GROUND OF REJECTION TO BE REVIEWED ON APPEAL	7
VII.	ARGUMENT	8
VIII.	CLAIMS APPENDIX	13
IX.	EVIDENCE APPENDIX	18
X.	RELATED PROCEEDINGS APPENDIX	19

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

I. REAL PARTY IN INTEREST

The real parties in interest in the above-identified application are two individuals, Hideki Koike, residing in Suginami-ku, Tokyo, Japan, and Tetsuji Takeda, residing in Chofu-shi, Tokyo, Japan, who are the named inventors of the present application.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

II. RELATED APPEALS AND INTERFERENCES

None.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

III. STATUS OF CLAIMS

Claims 1-6, 8-21, and 23-26 are pending in this case. All of these claims (Claims 1-6, 8-21, and 23-26) have been finally rejected and appealed.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

IV. STATUS OF AMENDMENTS

There are no outstanding amendments to this application.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claims 1 and 26 are independent claims. Claims 2-6, 8-21, and 23-25 depend from Claim 1. Claim 1 is directed to a log file protection system, and Claim 26 is directed to a log file protection method.

The subject matter of Claims 1 and 26 is directed to protecting a log file which records the operations of a computer system. In the prior art, for example, a server computer may be associated with a log file that records computer system operations of the server, such as deletion of a file on the server. Thus, even if an intruder could delete a file on the server, so long as its associated log file is protected from unauthorized alteration or deletion, an administrator of the server could determine (based on the log file) that the file has been deleted on the server. If, however, the log file itself is altered or deleted, to thereby erase the trace of an intruder action, then the server administrator will not even know whether, or what type of, unauthorized action has taken place. It is therefore imperative to maintain the integrity of a log file, and the present invention as recited in Claims 1 and 26, summarized below, is directed to achieving this goal.

Claim 1 recites a log file protection system for protecting log files in which computer system operations have been recorded. The system comprises generally three elements: (1) "log file creation means which create a plurality of identical log files which record the operations of said computer system," (2) "alteration detection means which periodically monitor said plurality of identical log files for alteration or deletion," and (3) "restoration means which restore an altered or deleted log file by replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files when the altered or deleted log file is detected by said alteration detection means." The "log file creation means" are described in page 4, lines 9-19 of the specification in reference to FIGURE 1(b). The "alteration detection means" are described in page 4, lines 20-25 and page 5, lines 3-6 of the specification in reference to FIGURE 2. The

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

"restoration means" are described in page 4, lines 26-31 of the specification in reference to FIGURE 3.

Claim 26 recites a method that generally corresponds to the system recited in Claim 1. Specifically, Claim 26 is directed to a log file protection method for protecting log files in which computer system operations have been recorded, and the method includes generally three steps: (a) creating a plurality of identical log files which record the operations of said computer system, (b) periodically monitoring said plurality of identical log files for alteration or deletion, and (c) restoring the altered or deleted log file by replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files when the altered or deleted log file is detected in said periodic monitoring step. Step (a) is described in page 4, lines 9-19 of the specification in reference to FIGURE 1(b), step (b) is described in page 4, lines 20-25 and page 5, lines 3-6 of the specification in reference to FIGURE 2, and step (c) is described in page 4, lines 26-31 of the specification in reference to FIGURE 3.

Some of the characteristic features of the system and method as recited in Claims 1 and 26, respectively, are the creation of "a plurality of identical log files which record the operations of [a] computer system," "periodically monitoring said plurality of identical log files for alteration or deletion," and replacing the altered or deleted log file "with an unaltered log file from the plurality of identical log files."

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

In the final Office Action mailed February 23, 2005, all pending claims (Claims 1-6, 8-21, and 23-26) were finally rejected based on a single ground, under 35 U.S.C. § 103(a), as being unpatentable over Shen (U.S. Patent No. 6,611,850) in view of Falkner (U.S. Patent No. 5,713,008).

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

VII. ARGUMENT

Rejection under 35 U.S.C. § 103(a), over (U.S. Patent No. 6,611,850) in view of (U.S. Patent No. 5,713,008).

As described above in Section V above, the present invention as recited in Claims 1 and 26 is directed to protecting a log file which records the operations of a computer system.

In Claim 1, a log file protection system of the invention comprises "log file creation means," "alteration detection means," and "restoration means." The log file creation means creates "a plurality of identical log files which record the operations of [a] computer system." The alteration detection means then "periodically monitors" the "plurality of identical log files" for alteration or deletion. When the alteration detection means detects an altered or deleted log file (among the plurality of identical log files), the restoration means restores the altered or deleted log file by replacing it with an unaltered log file obtained from the "plurality of identical log files." Thus, according to the invention recited in Claim 1, a plurality of identical log files which record computer operations are created and periodically monitored so that even if one of the identical log files should be altered or deleted, an altered or deleted log file can be replaced with another of the identical log files that has not been altered or deleted. The invention is based on the reality that an intruder, even if he/she could alter or delete one log file, is unlikely to be able to alter or delete all of the plurality of identical log files at the same time. (An intruder will not even know whether or how many of a plurality of identical log files are stored.) Therefore, as long as at least one of the identical log files remains unaltered and undeleted, this unaltered and undeleted log file can be used to replace any log file that has been altered or deleted, to thereby maintain the integrity of the identical log files as a whole.

Claim 26 is a method claim corresponding to the system recited in Claim 1, and thus is also characterized by the features of: creating "a plurality of identical log files which record the

operations of [a] computer system," "periodically monitoring" the "plurality of identical log files" for alteration or deletion, and replacing an altered or deleted log file with an unaltered log file from the "plurality of identical log files."

Applicants respectfully point out that Shen and Falkner cited against the present application, either alone or in combination, do not disclose or suggest the claimed features directed to (1) creating a plurality of identical log files which record the operations of a computer system, (2) periodically monitoring the plurality of identical log files for alteration or deletion, and (3) replacing an altered or deleted log file with an unaltered log file from the plurality of identical log files. Accordingly, Claims 1 and 26 of the present application are allowable in view of Shen and Falkner.

Specifically, Shen is not even related to a "log file" protection system, but rather is related to a conventional file backup/restore method. The present invention is directed to "protecting a plurality of *log files in which computer system operations have been recorded*" (Claims 1 and 26, emphasis added), which is different from Shen, directed to protecting a regular (non-log) file. As described above, maintaining the integrity of a log file is imperative (as compared to maintaining the integrity of regular files) because if the log file itself is altered or deleted, the trace of an intruder action is erased, and the computer administrator will not even know whether or what type of unauthorized action has taken place. On the other hand, if a regular file is altered or deleted, the trace of such intruder action is at least recorded in a log file, and thus the computer administrator can take a remedial action (e.g., restoring the regular file using a backup file). The distinction between protecting a log file and protecting a regular file is important to note, since conventional methods of making backup copies for regular files, as described in Shen, completely fail to address any need that is specific to maintaining the integrity of a log file, such

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

as the need to create and monitor *a plurality of identical log files* so that even if one of them should be altered or deleted there will remain at least one unaltered and undeleted log file.

Furthermore, though Shen teaches creating a plurality of backup files for each regular file, these backup files are created at different times and therefore are *not* identical to each other. Specifically, Shen describes:

> [T]he backup/restore control apparatus...includes...a "backup generation control means"...*to generate a backup copy at pre-set timing every time the designated file(s)* selected during the above-mentioned "backup file selecting means" *is/are created or updated.*

(Col. 5, lines 9-17, emphasis added.)

Shen teaches creating backup files at different times ("every time the designated file is created or updated") so that if any file is corrupted with a virus then the corrupted file can be replaced with a backup file that was stored prior to the time of corruption. To that end, Shen employs a "generation management unit 215 to manage the past status of these file(s)." (Col. 12, lines 28-32). More specifically, Shen describes:

> [T]he third objective [of the invention] is, to enable easy restoration of the original file(s) *to a state of designated time period backing from the current time*, using the backed-up file(s).
>
> Then, the fourth objective is, while this invention makes possible to easily restore the files to a state of designated time period backing from the current time, to enable *the management of past state of these files using the backed-up copy[ies].*

(Col. 2, lines 58-65, emphasis added.)

> By this method of taking a backup for all the modified file has the following advantage. That is, even if a file was infected by a virus that cannot be detected by a virus checker, *it is possible to restore back to a version of that file before getting infected.* But then, *since there may be many versions (generations) of the backed-up files*, it is very difficult to find a particular version, so in this form of implementation, a pre-defined "time period" is set at backup information setting unit 211, and restore the designated file.

(Col. 16, lines 39-47, emphasis added.)

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

In short, in Shen, a backup file is created "every time the designated file is created or updated," and therefore "many versions (generations) of the backed-up files" may be created over time, which obviously are *not* identical to each other.

Accordingly, Shen does not teach or suggest (1) creating a plurality of identical log files which record the operations of a computer system, as recited in Claims 1 and 26 of the present application. To the contrary, Shen explicitly teaches creating "many versions (generations)" of backup files. As such, Shen actually teaches *away* from creating "a plurality of *identical* log files" as recited in Claims 1 and 26.

Furthermore, Shen does not at all teach or suggest: (2) periodically monitoring the plurality of identical log files for alteration or deletion, nor (3) replacing an altered or deleted log file with an unaltered log file from the plurality of identical log files, as recited in Claims 1 and 26, either. Rather, in Shen:

> [A]n "integrity judgment process" will judge the integrity of the designated file when making a backup copy of such file during the "backup copy generation process," and only if the result of above-mentioned "integrity judgment process" prove to be positive (i.e., not infected by a virus or destroyed,) then it will generate a backup copy of the designated file.

(Col. 3, line 66-Col. 4, line 6.)

In other words, Shen monitors only the "designated file" (i.e., the original regular file) to see if it is "infected by a virus or destroyed" and, if not, creates a backup copy for this designated file (i.e., if the original regular file is infected by a virus, its backup copy will not be created). Shen only monitors the integrity of the "designated [original] file"; it is not at all concerned with monitoring the integrity of any *backup copy* of the designated file to see if the backup copy has been infected or destroyed, let alone monitoring a plurality of identical backup copies (partly because Shen does not create a plurality of identical backup copies to start with, as discussed above). As such, Shen does not teach or suggest periodically monitoring a *plurality of identical*

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

log files for alteration or deletion, nor replacing an altered or deleted log file, if found, with an unaltered log file from the plurality of identical log files, as recited in Claims 1 and 26.

Based on the foregoing reasons, it is respectfully submitted that Claims 1 and 26 are allowable over Shen.

With respect to Falkner, applicants note that the Office relied on Falkner only for the teaching of a conventional log file. ("[A] filesystem log file is provided for storing records of filesystem transactions invoked by the computer." Abstract.) Therefore, Falkner does not disclose or suggest: (1) creating a plurality of identical log files which record the operations of a computer system, (2) periodically monitoring the plurality of identical log files for alteration or deletion, and (3) replacing an altered or deleted log file with an unaltered log file from the plurality of identical log files, as recited in Claims 1 and 26. Consequently, Falkner cannot cure the deficiency of Shen, and therefore Shen and Falkner, even in combination, do not render the subject matter recited in Claims 1 and 26 obvious. Accordingly, Claims 1 and 26 are allowable in view of Shen and Falkner.

Claims 2-6, 8-21, and 23-25 are all dependent from Claim 1, and therefore are allowable for at least the same reasons why Claim 1 is allowable.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

VIII. CLAIMS APPENDIX

1. (Previously presented) A log file protection system for protecting log files in which computer system operations have been recorded, comprising:

log file creation means which create a plurality of identical log files which record the operations of said computer system;

alteration detection means which periodically monitor said plurality of identical log files for alteration or deletion; and

restoration means which restore the an altered or deleted log file by replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files when the altered or deleted log file is detected by said alteration detection means.

2. (Previously presented) The log file protection system of Claim 1, wherein said log file creation means create said plurality of identical log files in parallel, using identical information.

3. (Previously presented) The log file protection system of Claim 1, further comprising hiding means which hide all but one of the plurality of identical log files.

4. (Original) The log file protection system of Claim 3, wherein said hiding means periodically re-hide said hidden log files in different locations.

5. (Previously presented) The log file protection system of Claim 3, wherein said hiding means re-hide said hidden log files in

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

different locations, when alteration or deletion is detected by said alteration detection means.

6. (Previously presented) The log file protection system of Claim 5, further comprising means which perform additional processing, when alteration or deletion is detected by said alteration detection means.

7. (Canceled)

8. (Previously presented) The log file protection system of Claim 1, further comprising means which perform additional processing, when alteration or deletion is detected by said alteration detection means.

9. (Previously presented) The log file protection system of Claim 2, further comprising means which perform additional processing, when alteration or deletion is detected by said alteration detection means.

10. (Previously presented) The log file protection system of Claim 2, further comprising hiding means which hide all but one of the plurality of identical log files.

11. (Previously presented) The log file protection system of Claim 10, further comprising means which perform additional processing, when alteration or deletion is detected by said alteration detection means.

12. (Previously presented) The log file protection system of Claim 10, wherein said hiding means re-hide said hidden log files in different locations, when alteration or deletion is detected by said alteration detection means.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

13. (Previously presented) The log file protection system of Claim 12, further comprising means which perform additional processing, when alteration or deletion is detected by said alteration detection means.

14. (Previously presented) The log file protection system of Claim 10, wherein said hiding means periodically re-hide said hidden log files in different locations.

15. (Previously presented) The log file protection system of Claim 14, further comprising means which perform additional processing, when alteration or deletion is detected by said alteration detection means.

16. (Previously presented) The log file protection system of Claim 14, wherein said hiding means re-hide said hidden log files in different locations, when alteration or deletion is detected by said alteration detection means.

17. (Previously presented) The log file protection system of Claim 16, further comprising means which perform additional processing, when alteration or deletion is detected by said alteration detection means.

18. (Previously presented) The log file protection system of Claim 3, further comprising means which perform additional processing, when alteration or deletion is detected by said alteration detection means.

19. (Previously presented) The log file protection system of Claim 4, further comprising means which perform additional processing, when alteration or deletion is detected by said alteration detection means.

20. (Previously presented) The log file protection system of Claim 4, wherein said hiding means re-hide said hidden log files in

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

different locations, when alteration or deletion is detected by said alteration detection means.

21. (Previously presented) The log file protection system of Claim 20, further comprising means which perform additional processing, when alteration or deletion is detected by said alteration detection means.

22. (Canceled)

23. (Previously presented) The log file protection system of Claim 1, wherein said alteration detection means monitor said log files by using fingerprint data generated based on the entire content of the log file.

24. (Previously presented) The log file protection system of Claim 1, wherein said restoration means restore the altered or deleted log file automatically.

25. (Previously presented) Recording media which stores a program capable of implementing the log file protection system according to any of Claims 1-6, 8-21 or 23-24 on a computer system.

26. (Previously presented) A log file protection method for protecting log files in which computer system operations have been recorded, comprising:

(a) creating a plurality of identical log files which record the operations of said computer system;

(b) periodically monitoring said plurality of identical log files for alteration or deletion; and

(c) restoring the altered or deleted log file by replacing the altered or deleted log file with an unaltered log file from the plurality

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

of identical log files when the altered or deleted log file is detected in said periodic monitoring step.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

IX. EVIDENCE APPENDIX

None.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

X. RELATED PROCEEDINGS APPENDIX

None.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS[PLLC]

Shoko I. Leek
Registration No. 43,746
Direct Dial No. 206.695.1780

I hereby certify that this correspondence is being deposited in triplicate with the U.S. Postal Service in a sealed envelope as first class mail with postage thereon fully prepaid and addressed to Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the below date.

Date: September 23, 2005

SIL:jam

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100